0368-4283: Space-Bounded Computation 27/3/2018 – Lecture 4

Combinatorial Constructions of Expanders. The Zig-Zag product

Amnon Ta-Shma and Dean Doron

We want to construct an *explicit* family of D-regular expanders with spectral gap as large as possible, or, at least, expanders with constant spectral gap and constant degree.

Definition 1. *Let $\mathcal{G} = \{G_k\}_{k\in\mathbb{N}}$ be a family of (N_k, D_k)-graphs. We say $\mathcal{G}$ is* explicit *if for every k, $v \in [N_k]$ and $i \in [D_k]$, $Rot_{G_k}(v,i)$ can be computed in time* $\mathrm{poly}(N_k, D_k)$*. We say $\mathcal{G}$ is* fully explicit *if $Rot_{G_k}(v,i)$ can be computed in time* $\mathrm{poly}(\log N_k, \log D_k)$ *(that is, polynomial-time in the input length).*

Non-explicitly, most regular graphs are good expanders.

Theorem 2 ([1])**.** *Let n, $d \geq 3$. If G is a uniformly random d-regular undirected graph than with high probability (which tends to 1 as n grows to infinity), $\bar{\lambda}(G) \leq \frac{2\sqrt{d-1}}{d} + o(1)$.*

The above is nearly tight. Alon and Boppana proved that for every family $\{G_n\}$, where G_n is a d-regular graph over n vertices, $\bar{\lambda}(G) \geq \frac{2\sqrt{d-1}}{d} - o(1)$ [2]. Graphs that achieve $\bar{\lambda}(G) = \frac{2\sqrt{d-1}}{d}$ are called *Ramanujan*.

There are very good number-theoretic constructions which are very explicit but hard to analyse. For instance, for a prime q consider the graph $G = (V = \mathbb{F}_q, E)$ where $x \in \mathbb{F}_q^\star$ is connected to $x+1$, $x-1$ and x^{-1} and 0 is connected to itself, 1 and $q-1$. The graph is 3-regular, fully explicit, and has. constant spectral gap, but the proof is not easy. There are also explicit Ramanujan graphs.

We will see a combinatorial construction, following [3] which can be analysed with basic math. The main advantage of the combinatorial construction will be revealed later, when we use it in Reingold's algorithm (and variants) to derandomized the probabilistic algorithm for USTCON.

1 Cayley Graphs over Abelian groups

Let H be a finite group. A subset $S \subseteq H$ is *symmetric* if $g \in S$ iff $g^{-1} \in S$.

Definition 3. *Let H be a finite group and let $S \subseteq H$ be symmetric. The Cayley graph $Cay(H,S)$ is the graph whose vertices are labeled with the elements from H and (a,b) is an edge iff $a = bs^{-1}$ for some $s \in S$.*

The graph is $|S|$-regular. If S is closed under inverse the graph is undirected. We will only analyse the simple Abelian case. The non-Abelian case is much more interesting and can lead to degree D Ramanujan graphs.

We consider two natural examples of Cayley graphs:

1. The undirected cycle over n vertices: $H = \mathbb{Z}_n$, $S = \{-1, 1\}$.
2. The n-dimensional hypercube: $H = \mathbb{Z}_2^n$, $S = \{e_i : i \in [n]\}$, where e_i is the vector which is 1 in the i-th coordinate and 0 elsewhere.

If we construct a Cayley graph from a finite Abelian group, the eigenvectors are the characters of the group and the eigenvalues can be described quite simply:

Lemma 4. *Let H be a finite Abelian group and let $\chi : H \to \mathbb{C}$ be a character of H. Let $S \subseteq H$ be symmetric and let A be the normalized adjacency matrix of $Cay(H, S)$. Then, $\chi \in \mathbb{C}^H$ is an eigenvector of A with eigenvalue $\lambda = \frac{1}{|S|}\langle \chi, S \rangle$, where we treat S as a vector in $\{0,1\}^H$.*

Proof. We simply consider the i-th coordinate of $A\chi$, which is

$$\begin{aligned}(A \cdot \chi)(i) &= \sum_j A[i,j]\chi(j) = \frac{1}{|S|} \sum_{j: ji^{-1} \in S} \chi(j) \\ &= \frac{1}{|S|} \sum_s \chi(si) = \frac{1}{|S|} \sum_s \chi(s)\chi(i) = \frac{1}{|S|}\langle \chi, S \rangle \cdot \chi(i).\end{aligned}$$

□

We can conclude that the eigenvalues $\langle \chi, S \rangle$ are *all* the eigenvalues of A, as every character is an eigenvector, they are linearly independent and there are exactly $|H|$ of them (you can try proving it yourself, or see the above reference). Observe that the eigenvectors of $Cay(H, S)$ are *independent* of the set S.

Notice that with logarithmic degree we can get constant gap. The obvious question is whether we can get constant degree expanders with Cayley graphs. It turns out that with Abelian groups we cannot, however there are infinite families of constant degree Cayley expanders over non-Abelian groups but we will not cover them in the course.

Our next goal is to achieve a combinatorial construction of constant degree expanders.

2 Rotation maps

A *labelling* of a D-outregular graph G is an assignment of a number in $[D]$ to every edge of G such that the edges exiting every vertex have distinct labels. We say a labelling is *consistent* if for every vertex all incoming edges have distinct labels. That is similar to labelling undirected graphs, and it can be shown that every regular directed graph *can* be consistently labeled. Although working with consistently labeled graph suffices for our current application, we consider a more general notion of labelling, a *two-way labelling*, where every edge has two labels – one as an outgoing edge and one as an ingoing edge. A graph together a two-way labelling can be specified by a *rotation map*.

Definition 5. *Let G be a directed D-regular over N vertices. A rotation map for G, $Rot_G : [N] \times [D] \to [N] \times [D]$ is defined as follows: $Rot_G(v, i) = (w, j)$ if the i-th outgoing edge from v leads to w, and this edge is the j-th incoming edge of w.*

Notice that the rotation function is always a *permutation*. If G is *undirected*, we can view it as a directed graph by replacing every undirected edge $\{u, v\}$ with two directed edges (u, v) and (v, u). We can insist that the outgoing label of (u, v) is the same as the incoming label of (v, u). The resulting rotation map Rot of such a two-way labelling is not only a permutation but also an *involution*, namely Rot^2 is the identity.

Using two-way labelling instead of ordinary labelling has two advantages. First, even though every regular directed graph has a consistent labelling, it seems to be infeasible finding it in logspace.

Second, some properties such as consistent labelling or being undirected may not be preserved under some products so it would be easier to work with a more robust definition that does not assume those properties.

Example 6. *(Squaring) Say G is an (N, D, λ) graph with rotation map Rot. Then G^2 is a (N, D^2, λ^2) graph with rotation map Rot′ where $Rot'(v; a_1, a_2) = (v'', (a'_2, a'_1)$ where $Rot(v, a_1) = (v', a'_1)$, $Rot(v', a_2) = (v'', a'_2)$.*

Example 7. *(Tensoring) Say G is an (N, D, λ) graph with rotation map Rot. Then $G \otimes G$ is a (N^2, D^2, λ) graph with rotation map Rot′ where $Rot'((v_1, v_2); a_1, a_2) = ((v'_1, v'_2), (a'_1, a'_2)$ where $Rot(v_1, a_1) = (v'_1, a'_1)$, $Rot(v_2, a_2) = (v'_2, a'_2)$.*

3 The Zig-Zag Product

3.1 The overall idea

We start with some constant sized $(N_0, D_0, \lambda_0 < 1)$-graph G. Then:

1. We improve $\bar{\lambda}(G)$ by powering – G^2. The drawback: Powering blows-up the degree.
2. We increase the number of vertices by tensoring – $G \otimes G$. Tensoring preserves $\bar{\lambda}(G)$ however also blows-up the degree.

We thus need a new graph operation that would:

- roughly preserve the number of vertices (since we can increase it with tensoring),
- roughly preserve $\bar{\lambda}(G)$ (since we can square), and,
- decreases the degree.

Then, morally, we can repeatedly apply:

1. Tensoring, to increase the number of vertices.
2. Powering, to increase the spectral gap.
3. The new operation that reduces the degree.

And so, we can potentially obtain an infinite family of constant degree expanders.

3.2 The replacement product

We begin with a product that takes a "large" D_1-regular undirected graph $G = (V, E)$ over N vertices and a "small" D_2-regular graph over D_1 vertices H and produces a $(D_2 + 1)$-regular graph over ND_1 vertices. The replacement product $G(\circledR)H$ goes as follows:

- Replace every vertex of G with a copy of H, called a "cloud" (and has its "intra-cloud edges"). For every $v \in [N]$ and $i \in [D_1]$, (v, i) is then a vertex of $G(\circledR)H$.

- For $e = \{u, v\} \in E$ such that v is the i-th neighbor of u and u is the j-th neighbor of v, we have an "inter-cloud" edge $\{(u, i), (v, j)\}$.

Formally, we can describe the rotation map $Rot_{G\circledR H}((v, i), k)$ where $k \in \{0, 1, \ldots, D_2\}$ as follows:

1. Let $(v', i') = Rot_G(v, i)$.
2. If $k > 0$, let $(i', k') = Rot_H(i, k)$.
3. If $k = 0$ then output $((v', i'), 0)$. Else, output $((v, i'), k')$.

3.3 The zig-zag product and its analysis

We now wish to "short-circuit" steps on the replacement product graph. Again, let G be an (N, D_1, λ_1)-graph and let H be a (D_1, D_2, λ_2)-graph, and we think of $D_2 \ll D_1$ and of H as an expander. The zig-zag product $G\circledcirc H$ goes as follows:

- The vertex set is the vertex set of $G\circledR H$.
- There is an edge $\{(u, i), (v, j)\}$ if (v, j) can be reached from (u, i) by taking a step in the u-cloud, then a step between the clouds and then a step in the v-cloud. That is, we take one intra-cloud step, one inter-cloud step and one intra-cloud step.

Is the above well-defined? I.e., is the graph an undirected one? Next, observe that the graph is D_2^2-regular. Is it connected?

Let us formally describe the rotation map $Rot_{G\circledcirc H}((v_1, v_2), (i_1, i_2))$:

1. Let $(v_2', i_1') = Rot_H(v_2, i_1)$.
2. Let $(v_1', v_2'') = Rot_G(v_1, v_2')$.
3. Let $(v_2''', i_2') = Rot_H(v_2'', i_2)$.
4. Output $((v_1', v_2'''), (i_2', i_1'))$.

We can also view the zig-zag product in the following way: We start with some vertex of $G\circledR H$ and are given two instructions $i_1, i_2 \in [D_2]$. The graph H is the one that dictates the intra-cloud steps, whereas the intra-cloud step is deterministic.

The zig-zag product roughly inherits the degree of the smaller graph, which is good. But what about the spectral gap? Does it preserve it?

Theorem 8. *Let G be an $(N, D_1, \lambda_1 = 1 - \gamma_1)$ and let H be a $(D_1, D_2, \lambda_2 = 1 - \gamma_2)$. Then, $G\circledcirc H$ is a $(ND_1, D_2^2, f(\lambda_1, \lambda_2))$ where $\gamma = 1 - f(\lambda_1, \lambda_2) \geq \gamma_1\gamma_2^2$.*

Proof. We let A be the transition matrix of G, B be the transition matrix of H and M be the transition matrix of $G\circledcirc H$. Same as we did for in the analysis of the derandomized squaring product, let $\dot{A}$ be the permutation corresponding to Rot_G and let $\tilde{B} = I_N \otimes B$. Then,

$$M \;=\; \tilde{B}\dot{A}\tilde{B}.$$

Again, write $B = (1-\lambda_2)\frac{1}{D_1}J + \lambda_2 E$ for some E with $\|E\| \leq 1$ and denote $\tilde{J} = I_N \otimes \frac{1}{D_1}J$ and $\tilde{E} = I_N \otimes E$, so $\tilde{B} = (1-\lambda_2)\tilde{J} + \tilde{E}$, and so

$$\begin{aligned} M &= ((1-\lambda_2)\tilde{J} + \lambda_2\tilde{E})\dot{A}((1-\lambda_2)\tilde{J} + \lambda_2\tilde{E}) \\ &= \gamma_2^2 \tilde{J}\dot{A}\tilde{J} + F, \end{aligned}$$

where $F = \lambda_2(1-\lambda_2)(\tilde{J}\dot{A}\tilde{E} + \tilde{E}\dot{A}\tilde{J}) + \lambda_2^2\tilde{E}\dot{A}\tilde{E}$. As $\|\tilde{E}\|, \|\dot{A}\|, \|\dot{J}\| \leq 1$ we get

$$\|F\| \leq 2\lambda_2(1-\lambda_2) + \lambda_2^2 = 2\lambda_2 - \lambda_2^2 = 1 - (1 - 2\lambda_2 + \lambda_2^2) = 1 - \gamma_2^2.$$

Also, observe that $\tilde{J}\dot{A}\tilde{J} = A \otimes \frac{1}{D_1}J$ (why?). Thus,

$$\bar{\lambda}(G \textcircled{z} H) \leq \gamma_2^2 \cdot \bar{\lambda}(G) \cdot \left\| \frac{1}{D_1}J \right\| + \|F\| = \gamma_2^2\lambda_1 + 1 - \gamma_2^2$$

so $1 - \bar{\lambda}(G \textcircled{z} H) \geq \gamma_2^2(1-\lambda_1) = \gamma_2^2\gamma_1$. □

4 Constructing constant-degree expanders

4.0.1 An explicit family of expanders

Fix a large enough constant D. We start with a constant-sized expander.

Theorem 9. *There exists a $(D^4, D, \frac{1}{8})$-graph.*

Although a brute-force search is possible (why?), we will give an explicit construction of such an expander in the homework assignment.

Let H be the $(D^4, D, \frac{1}{8})$-graph and let $G_1 = H^2$. For $k \geq 1$, define

$$G_{k+1} = G_k^2 \textcircled{z} H$$

Lemma 10. *For every $k \geq 1$, G_k is a $(D^{4k}, D^2, \frac{1}{2})$-graph.*

Proof. By induction on k. For $k = 1$ it is guaranteed by Theorem 4.0.1 and the squaring. Now, assume G_k is a $(D^{4k}, D^2, \frac{1}{2})$-graph. Thus, G_k^2 is a $(D^{4k}, D^4, \frac{1}{4})$-graph. Recall that H is a $(D^4, D, \frac{1}{8})$-graph, so by the zig-zag analysis, G_{k+1} is a

$$(D^{4(k+1)}, D^2, 1-\gamma)$$

graph, for $\gamma \geq (1-\frac{1}{8})^2(1-\frac{1}{4}) > \frac{1}{2}$, as desired. □

How explicit is the family $\{G_k\}_k$? Say we computed the rotation map of G_k and wish to compute the rotation map of G_{k+1}. Recall that $Rot_{G_{t+1}}((v,a),(i_1,i_2))$ where $v \in [D^{4k}]$, $a \in [D^4]$ and $i_1, i_2 \in [D]$, is given by:

1. Compute $(a', i_1') = Rot_H(a, i_1)$, where $a' \in [D^4]$ and $i_1' \in [D]$.
2. Compute $(v', a'') = Rot_{G_k^2}(v, a')$, where $v' \in [D^{4k}]$ and $a'' \in [D^4]$.

3. Compute $(a''', i'_2) = Rot_H(a'', i_2)$.

4. Output $((v', a'''), (i'_2, i'_1))$.

To compute $(v', a'') = Rot_{G_k^2}(v, a')$, denote $a' = (a'_1, a'_2) \in [D^2]^2$, compute $(w, a''_1) = Rot_{G_k}(v, a'_1)$, $(v', a''_2) = Rot_{G_k}(w, a'_2)$ and set $a'' = (a''_2, a''_1)$.

We want to prove that our family is indeed explicit. Let $T(k)$ be the time needed to compute Rot_{G_k}. Thus,

$$T(k) \;=\; 2T(k-1) + O(1),$$

where the $O(1)$ factor stands for the computations of Rot_H. Thus, $T(k) = O(2^k)$ and since the number of vertices is $N = D^{4k}$, $T(k) = O(2^{\frac{1}{4}\log_D N}) = \text{poly}(N)$.

4.0.2 A fully explicit family of expanders

Can we do better in terms of explicitness? Let H a $(D^8, D, \frac{1}{8})$-graph and let $G_1 = H^2$. For $k \geq 1$, define

$$G_{k+1} \;=\; (G_k \otimes G_k)^2 \textcircled{z} H.$$

Lemma 11. *For every $k \geq 1$, G_k is a $(N_k, D^2, \frac{1}{2})$-graph where $N_k \geq D^{2^k}$.*

Proof. Assume G_k is an $(N_k, D^2, \frac{1}{2})$-graph. Thus, $G_k \otimes G_k$ is an $(N_k^2, D^4, \frac{1}{2})$-graph and so $(G_k \otimes G_k)^2$ is an $(N_k^2, D^8, \frac{1}{4})$-graph. Recall that H is a $(D^8, D, \frac{1}{8})$-graph, so by the zig-zag analysis, G_{k+1} is a

$$(N_{k+1} = N_k^2 D^8, D^2, 1-\gamma)$$

graph, for $\gamma \geq (1-\frac{1}{8})^2(1-\frac{1}{4}) > \frac{1}{2}$. Finally, note that $N_{k+1} \geq \left(D^{2^k}\right)^2 D^8 \geq D^{2^{k+1}}$, as desired. □

Again, we wish to examine the construction's time complexity. We skip explicitly writing all the steps in computing Rot_{G_k}, but do it yourself! The recurrence relation for the time complexity is now

$$T(k) \;=\; 4T(k-1) + O(1),$$

giving $T(k) = O(4^k)$. As $N \geq D^{2^k}$ we get $T(k) = \text{poly}(\log N)$, as desired. This family is fully explicit.

References

[1] Joel Friedman. *A proof of Alon's second eigenvalue conjecture and related problems.* American Mathematical Soc., 2008.

[2] Alon Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207–210, 1991.

[3] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Annals of mathematics*, pages 157–187, 2002.